Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 12 November 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Journal News reports hundreds of people looking for work at an event organized last month by the New Jersey Department of Labor, unknowingly provided personal financial information to a fraudulent company. (See item 5)
- Reuters reports the Senate has approved a measure that would let cargo pilots carry guns, just days after authorities warned new attacks could be launched against American targets using that type of aircraft. (See item 11)
- The Australian Associated Press reports hackers have reportedly accessed top−secret files inside the Australian Department of Defense, gaining an unauthorized access to computer systems. (See item 24)
- Internet Security Systems has raised Alertcon to Level 2 due to vulnerabilities or threats to computer networks that require assessment and corrective action. Refer to Internet Alert Dash Board.
- Security Focus has raised ThreatCon to Level 2, citing a need for increased vigilance. Refer to Internet Alert Dash Board.

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *November 08, Reuters* — **Power blackout in Chile.** Most of Chile lost power in a major blackout on Friday, November 7. The blackout occurred in the evening, snarling rush hour traffic in its capital, Santiago, which is home to 5 million people or one third of the country's population. **The blackout began at about 7:20 p.m., and power started coming back on at 9:00 p.m., National Electricity Superintendent Sergio Espejo said. He said the country's central grid went down, but gave no other explanation for the blackout,** which was total in a large part of central Chile. He said investigations would begin when everything was normal. Television reports said power went out as far as Puerto Montt, a city about 600 miles south of Santiago, and in areas the same distance to the north.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2003_11_07_eng−reuters_pma_POWER−BLACKOUT−HITS−MOST−OF−CHILE&SMContentSet=0

2. *November 07, Reuters* — **Blackout report release set for November 18.** U.S. and Canadian investigators will release a report on Tuesday, November 18 detailing the cause of last August's massive power blackout, the U.S. Energy Department said on Friday, November 7. The U.S. Energy Department and its Canadian counterpart are probing what caused the August 14−15 electricity outage that left 50 million people in eight northeastern states and Canada in the dark. **The report "accesses conditions on the electric transmission grid that contributed to the blackout, outlines the actual physical cause of the outage, and discusses events and conditions that allowed the blackout to spread," the Energy Department said in a release.**
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2003_11_07_eng−reuters_pma_US−DOE−SAYS−WILL−RELEASE−BLACKOUT−REPORT−ON−NOV&SMContentSet=0

3. *November 07, Reuters* — **Duane Arnold nuke manually shut. The 580 megawatt Duane Arnold nuclear unit in Palo, IA, was manually shut Friday, November 7, due to "impure water" going into the reactor,** a spokesperson for the plant's operator said. John Lohman, of the Nuclear Management Company, was unable to provide restart information on the unit until the cause of the problem is determined. "This is the same issue as (earlier this week). We shut the plant down because, basically, 'bad water' was getting into the reactor," Lohman said. **Early Friday the U.S. Nuclear Regulatory Commission said in a daily report that the unit was manually tripped due to "high reactor coolant conductivity."** It had been operating at 45 percent of capacity when operators shut it. The unit had been previously shut on Monday, November 3, for condenser tube repairs.
Source: http://biz.yahoo.com/rm/031107/utilities_alliant_duanearnold_2.html

[Return to top]

Chemical Sector

4. *November 10, Associated Press* — **Work continues on barge leaking sulfuric acid.** Efforts continued on Monday to salvage a barge that capsized last week leaking sulfuric acid into a Texas City harbor. **Crews were pumping nitrogen gas into the barge to prevent explosive**

pockets of hydrogen gas from forming. Salvage slings and rigging also were being adjusted before an attempt is made to upright barge, which remains on its port side with its bow aground and stern afloat. The barge, which is operated by Martin Product Sales LLC, of Kilgore, TX, turned over in about 30 feet of water on November 5 after capsizing in the Texas City harbor two days earlier. **The tug was carrying 235,000 gallons of sulfuric acid.** Crews with the Environmental Protection Agency, the National Oceanic Atmospheric Administration and the Coast Guard were on site. **No injuries have been reported. The cause of the accident remains under investigation.**
Source: http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/221373 7

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *November 08, The Journal News (NY)* — **Job seekers revealed personal information in employment scam. Hundreds of people looking for work at an event organized last month by the New Jersey Department of Labor unknowingly provided personal financial information to a fraudulent company, the department said last week.** The job applicants gave Frisco, TX−based ELS Locators, also known as ELS Vending, a $42 fee along with their Social Security numbers, bank account numbers and credit card information. Jersey City Police Chief Ronald Buonocore said that he has since been notified by federal authorities that **the company was part of a multistate scheme to steal personal information. Hundreds of people already have been affected by the scam, which authorities believe has extended to 15 cities in eight states.** Detective Ronald Schmidt said the scam involved placing newspaper ads for people looking for work and promising they would make $18 an hour by dispatching trucks to vending machines that needed repair. They stole Social Security numbers and other personal information from these individuals when they filled out application forms, Schmidt said.
Source: http://www.nynews.com/newsroom/110803/d01a08scam.html

[Return to top]

Transportation Sector

6. *November 11, New York Times* — **A baggage lock for passengers and federal screeners. Airline passengers will be able to lock checked bags confidently again starting Wednesday, thanks to a new customer−service initiative between private enterprise and the Transportation Security Administration (TSA).** Several major luggage and lock retailers in the United States will announce on Wednesday the availability of new locks, made by various manufacturers, that TSA inspectors will be able to readily identify and open on checked bags selected for hand searches at airports. TSA screeners in airports around the country have

already been trained in using secure procedures to open the new certified locks when necessary, and relock them after inspecting bags. **"Literally since we began the process of screening every checked bag for explosives in December, one of the challenges has been the ability to get into bags without doing damage to them,"** said Brian Turmail, a spokesman for the TSA. **The system will ensure that passengers using the locks will not have to worry about a lock being broken or a locked bag being damaged if it is selected for hand inspection. It will also mean more peace of mind for passengers worried about reports of increased pilferage from unlocked bags.**
Source: http://www.nytimes.com/2003/11/11/business/11road.html

7. *November 10, Jackson Sun (TN)* — **Unsafe bridges should be closed or repaired. The Tennessee Department of Transportation (TDOT) Commissioner Gerald Nicely has declassifying millions of pages of state bridge inspection reports. The findings contained in those reports are startling. There are 22 unsafe bridges being kept open in West Tennessee, despite recommendations by TDOT that they be closed** −− 12 in Weakley County alone. Clearly, public safety demands that this information be made public. Now, it's time for county governments to act. Those bridges cited by TDOT should either be repaired or closed. It's understandable that counties are facing a budget crunch thanks to the state financial mess. And closing some of these bridges will inconvenience motorists, since they are vital to local transportation. But this is a project that should take top priority.
Source: http://miva.jacksonsun.com/miva/cgi−bin/miva?OPINION/opinion_story.mv+link=200311105546004

8. *November 10, BBC* — **UK airport fails security test. The UK's Edinburgh Airport is reported to have failed a recent undercover government security test. Plain clothed officers from the Department of Transport are understood to have managed to pass devices through the airport's x−ray machines and take them into the cabin of an airplane.** A spokesman for the transport department said it was within its rights to carry out such tests at any time, but would not confirm if this specific incident took place. British Airports Authority (BAA), which owns Edinburgh airport, would not comment on the details either, but said security is given the highest priority at all times. **A Scottish newspaper described the objects as "bomb−like" and reports that the devices had been hidden inside a laptop computer and a hairdryer before being put into luggage for the test last month.** Edinburgh, which handles almost seven million passengers a year, is part of the BAA, which also runs Glasgow, Aberdeen, Heathrow, Gatwick, Stansted and Southampton. Edinburgh Airport bosses promised to tighten security four years ago after explosives, guns and knives were carried undetected through checkpoints in a similar operation by Transport Department staff.
Source: http://news.bbc.co.uk/2/hi/uk_news/scotland/3256325.stm

9. *November 10, CNN* — **Straying plane prompts White House alert.** The Secret Service at the White House went on alert briefly Monday morning after an aircraft crossed into restricted airspace in what appeared to be an accidental violation. **The aircraft −− listed in federal aviation records as a four−seat, single−engine, propeller−driven Mooney M20E −− was intercepted and ordered to land. After receiving word of an unauthorized aircraft in the restricted District of Columbia airspace, armed Secret Service officers began patrolling the White House grounds, some with rifles and other firearms drawn. At no point did the Secret Service activate an internal White House alert system, which is used to inform the**

staff of possible security breaches or attacks. Fighter jets were scrambled to intercept the plane, and the pilot responded to instructions to change course. Another government source said the initial conclusion, based on the pilot's cooperation when contacted and intercepted, is that it was an inadvertent violation, as happens periodically.
Source: http://www.cnn.com/2003/US/South/11/10/plane.scare/index.htm l

10. *November 10, Associated Press* — **Tight budget, power issues postpone plan for new rail cars.** The Chicago Transit Authority (CTA) is postponing plans to purchase more than 700 new rail cars because of the agency's budget woes and delays in changing how the trains are powered. **The CTA plans to phase in a switch to alternating current (AC) electrical propulsion on all seven rapid−transit lines starting within about five years. Chicago has the last major transit agency in the United States that operates only on direct current (DC).** The agency's financial troubles delay the switch to AC power because the conversion requires the CTA to change its signal and communications systems to accommodate the 706 rail cars that will be purchased. **AC train motor systems have smoother acceleration and braking, which not only makes for a less bumpy ride, but a quieter one as well. Trains under the system also use power more efficiently, reducing operating and maintenance costs and the amount of wear and tear on the cars, said Paul Fish, CTA vice president of capital investment.** "Being the only transit agency left in the country that operates a DC propulsion system raises our costs significantly," Fish said.
Source: http://www.thetimesonline.com/articles/2003/11/10/roundups/r oundups/1101dbaa86b8b89886256dda005f0e85.txt

[Return to top]

Postal and Shipping Sector

11. *November 11, Reuters* — **Senate approves plan to arm cargo pilots.** The Senate approved a measure late on Monday that would let cargo pilots carry guns just days after authorities warned new attacks could be launched against American targets using that type of aircraft. **The Senate plan, first proposed last March by California Democrat Barbara Boxer and Kentucky Republican Jim Bunning, would permit cargo pilots to carry firearms and non−lethal stun guns as last−ditch options to deter any hijacking.** The measure would amend a law passed after the 2001 hijack attacks on New York and Washington that permits commercial airline pilots to carry guns on duty on a voluntary basis. **The House of Representatives included a provision earlier this month to arm cargo pilots in its version of the $60 billion Federal Aviation Administration reauthorization bill.** Until this month, most cargo security concerns had focused on mail and packages loaded aboard commercial airliners, not lumbering cargo jets that fly often at night and without passengers. **But the Bush administration said on Friday that recent intelligence suggests that cargo planes −− possibly seized overseas −− could be used against American targets, possibly inside the United States.** Cargo pilots had stepped up their warnings of potential security flaws in their industry since a man shipped himself by air cargo from New York to Texas earlier this fall.
Source: http://www.nytimes.com/reuters/politics/politics−security−co ngress−pilots.htm

[Return to top]

Agriculture Sector

12. *November 10, Pennsylvania Ag Connection* — **Rabies program. The costs of dealing with rabies are extremely high, and that's why a wildlife expert in Pennsylvania State University's College of Agricultural Sciences is working with the U.S. Department of Agriculture (USDA) to stop rabies from moving west out of Pennsylvania.** "Ohio doesn't have much raccoon rabies, it just has not gotten there yet," explains Gary San Julian, professor of wildlife resources. The USDA dropped fish meal pellets containing a raccoon rabies vaccine in September from low−flying aircraft in the multiple Pennsylvania counties. The baited zone extended approximately 60 miles into Pennsylvania and officials say the drops will move eastward in future years as funding permits. "The USDA Animal and Plant Health Inspection Service is attempting to establish a barrier stretching from the eastern Ohio and western Pennsylvania Lake Erie shoreline southward through West Virginia, Virginia and into northern Tennessee to reduce the risk of raccoon rabies spreading westward into the Midwest states," says San Julian. **"Rabies came into Pennsylvania so quickly from the south. It made a geographic jump in the 1960s that most people think it shouldn't have been able to make, and we need to stop it from making another big jump into the Midwest."**
    Source: http://www.pennsylvaniaagconnection.com/story−state.cfm?Id=6 9&yr=2003

13. *November 10, Biloxi Sun Herald* — **Disease leads fish farm to sustainable solution.** For several years, the SeaChick company, in Mississippi, had struggled to make a profitable business of tanks and ponds crowded with a striped bass hybrid. It seemed that as soon as one sickness filtered out, another would enter. **When a new bacteria known as streptococcus iniae swept through fish farms in the 1990s, an emergency meeting was called in the aquaculture community. Growers hoped to increase their use of the antibiotic amoxicillin. SeaChick went a different direction.** "What we had missed in this entire situation was the fact that we were creating a forest of cloned trees," said Don Robohm, president and founder of SeaChick. "All these common offspring were subject to the same genetic foibles and weaknesses of their parents." **At the bottom of SeaChick's series of channels, cleaning the scraps from the sick and healthy, was a pool of Nile tilapia. "These tilapia have been cleaning up our effluent. They've seen every disease that we've got. They don't catch it," Robohm said. And so, with a fish species already becoming known commercially as a good food fish, Robohm switched his stock.** Today, SeaChick raises healthy fish without using antibiotics, an anomaly in the world of aquaculture.
    Source: http://www.sunherald.com/mld/sunherald/news/local/7224530.ht m

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

14.

November 10, di−ve News — **Saboteur contaminates water supply at Ta' Kandja. Water supplies in 25 southern localities, in Malta, were suspended on Monday after the Water Service Corporation (WSC) discovered that the water in the Ta' Kandja galleries has been contaminated. A pipe used to supply chlorine for water purification was cut and substituted by a pipe supplying fuel.** "An unidentified person gained access to the chlorination room, where chlorine is pumped into water reservoirs for purification. Access to this room is easy because its doors are left open for ventilation. He cut off the pipe supplying chlorine, substituting it with fuel," said WSC chairman Michael Falzan. WSC chief Executive Officer Anthony Rizzo said that water supplies to certain localities were cut to check the contamination of water. "Around 15 liters of fuel were pumped into the sump full of water stored at Ta' Kandja pumping station during the weekend. Since fuel is lighter than water, a layer of fuel formed at the top and the water pumped to the reservoir was not contaminated," he added. **The WSC chairman said that the mastermind behind this act of sabotage is familiar with the water supplying systems. "At this point, we are not excluding anything and even the employees are being questioned by the police," he said.**
Source: http://www.di−ve.com/dive/portal/portal.jhtml?id=114070&pid= null

[Return to top]

Public Health Sector

15. *November 10, Scientist* — **Select agent regulations ammended. Scientists who work with select biological agents and toxins but who have not yet been issued certificates required by the U.S. Centers for Disease Control and Prevention (CDC) and the U.S. Department of Agriculture (USDA) can breathe easier now. As long as such researchers have submitted all necessary documentation to the government before a November 12 deadline, they can be issued provisional registration certificates if FBI background checks haven't been completed, according to Ted Jones, acting director of the CDC's Select Agent Program.** Under the select agent rule, researchers needing access to select agents, a collection of 80 bacteria, viruses, and toxins must undergo security assessments by the FBI and a lab inspection by the CDC or the USDA. Jones said last week that those labs whose paperwork is in order but that had not yet been inspected by the CDC would be given permission to continue working after the November 12 deadline. A USDA spokesperson said that labs wishing to work with select agricultural agents could receive a three−year certificate of registration without inspection. The background checks were to have been completed by June 12, but many of the 8000 background checks have not been completed.
Source: http://www.biomedcentral.com/news/20031110/06

16. *November 10, Mail & Guardian South Africa* — **Suspected Ebola outbreak kills nine in Congo.** An outbreak of the Ebola virus is believed to have claimed the lives of nine people in Congo. Spokesman Dr. Andrew Jamieson said a further three people appeared to have contracted the disease, although clinical samples collected in the field were still to be tested at a medical center in neighbouring Gabon to confirm the diagnosis. The area of the suspected outbreak, the Mbomo district of Cuvette−Ouest, is 700 km north of Congo's capital city Brazzaville and lies very close to the border with Gabon. **Jamieson said that according to media statements released by Congo's health ministry, the nine people who had died so far were all members of a group of hunters who ate meat collected from a wild boar found**

dead in the forest. Only one member of the hunting party survived the excursion, a young boy who refused to touch the game. Although still awaiting biological certification that the cause of death was infection with Ebola virus, the health ministry has re−issued advisory notices warning the populace of the risk of contracting the disease through infected meat. **Scientists believe that the Ebola outbreak which killed 120 people in the same region of Congo earlier this year was caused by infected monkey meat.**
Source: http://www.mg.co.za/Content/l3.asp?ao=23290

17. *November 10, American Heart Association* — **Heart disease following smallpox vaccination. The rate of adverse cardiac events was about 58 per 100,000 smallpox vaccinations in data collected between January and May 2003,** said Richard Schieber, of the U.S. Centers for Disease Control and Prevention (CDC). **Twenty−four cases of pericarditis, myocarditis, dilated cardiomyopathy, or acute coronary syndromes were identified among 37,876 U.S. civilian healthcare workers vaccinated.** Twenty−two patients had pericarditis or myocarditis. **The average interval from vaccination to illness was about 12 days.** Two of eight patients with acute coronary syndromes died. Five of the eight had three or more risk factors for, or a history of, coronary artery disease before vaccination. The American Heart Association said, **"In the past, cardiac complications after smallpox vaccination have been rare, but the majority of individuals undergoing vaccination in previous programs were children or young adults. Now that a large number of adults are receiving the vaccine, especially those in middle age who may have underlying heart disease, it will be important to carefully and continuously monitor the situation."**
Source: http://www.eurekalert.org/pub_releases/2003−11/aha−sdh102203 .php

18. *November 09, Associated Press* — **Bone ailment found in some SARS survivors. Hong Kong Hospital officials said Sunday that 49 Severe Acute Respiratory Syndrome (SARS) survivors are suffering from a degenerative bone disorder, a likely side−effect of the steroids used to treat them.** Many Hong Kong SARS patients were treated with an antiviral drug and high dosages of steroids, and some experts had warned that the regimen may be harmful. The Hong Kong Hospital Authority said in a statement that 49 of the 1,755 people who had contracted SARS in the territory have avascular necrosis, which hampers blood flow to the bone, leading to fractures. Researchers have also linked the steroid treatment to the occurrence of bone−weakening osteoporosis in some other survivors of severe acute respiratory syndrome, but the authority's statement made no mention of the disease.
Source: http://abcnews.go.com/wire/Living/ap20031109_392.html

[Return to top]

Government Sector

19. *November 11, Department of Homeland Security* — **Department of Homeland Security launches Operation ICE Storm. Top law enforcement and government officials have joined with the Department of Homeland Security to announce Operation ICE Storm, an unprecedented multi−agency initiative led by the Department's Immigration and Customs Enforcement (ICE) to combat human smuggling and the violence it has generated in Arizona and nationwide.** At a news conference in Phoenix on Tuesday morning, ICE Acting Assistant Secretary Michael J. Garcia laid out details of the effort, which includes the formation

of a task force made up of federal, state, and local agencies. Garcia pledged that the task force will use its broad range of authorities and resources to dismantle organized crime outfits that have turned human smuggling into a bloody but profitable venture. **ICE, as the largest investigative arm of Homeland Security, brings to bear a broad array of authorities and resources that make it uniquely qualified to lead the fight against human smuggling. ICE agents will combine immigration, smuggling, and financial investigative powers to attack the criminal rings from a variety of levels.** ICE's financial investigations expertise, for example, will allow the task force to follow the money trial in ways not previously possible.
Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0291.xml

20. *November 10, Federal Computer Week* — **Border agents with X−ray vision. The border agents in Otay Mesa, CA, are equipped with technology that allows them to virtually look inside a truck by capturing an image on a computer of what is there. That has proven to be an invaluable tool to inspect the 3,000 trucks heading from Mexico to the United States daily.** The search is conducted using the Vehicle and Cargo Inspection System (VACIS). U.S. Bureau of Customs and Border Protection officials have purchased 127 of these devices for about $1 million each and are using them at both the northern and southern borders to inspect the contents of trucks, railroad cars and ship containers. **There is also software that can analyze images to determine if there is something fishy about a vehicle's contents — a round object, for example, when everything else is square; a false wall that might hide contraband or illegal aliens; or material that shows up denser in the picture than the rest of the cargo.** The inspection takes seconds, and the image is stored in a computer database in the event of a problem later. Since it has been deployed, the system has inspected nearly two million commercial shipments, according to Douglas Browning, deputy commissioner for Customs and Border Protection, which is part of the Homeland Security Department.
Source: http://www.fcw.com/fcw/articles/2003/1110/cov−usvisit2−11−10 −03.asp

21. *November 10, National Journal's Technology Daily* — **Some Homeland Security activities remain unfunded. Despite President Bush's approval of the fiscal 2004 Homeland Security Department spending bill, more than 25 percent of federal homeland security activities remain unfunded,** a top Senate budget expert said Monday. Six weeks into fiscal year 2004, Congress has passed four of 13 departmental appropriations bills. **The Homeland Security appropriations was the first signed by Bush, but in fact that accounts for little more than half of administration−wide spending on homeland security,** said Bill Hoagland, budget and appropriations director in the Senate Majority Leader's office. Total fiscal 2004 federal spending on homeland security is expected to be $41.3 billion, Hoagland said at an Equity International homeland security conference. Only about two−thirds, or approximately $23.9 billion, of the total Homeland Security Department funding of $29.4 billion is for homeland security activities. **The remainder is for items such as regular operations of the Coast Guard and disaster response.**
Source: http://www.govexec.com/dailyfed/1103/111003tdpm1.htm

22. *November 10, National Journal's Technology Daily* — **Communications system proves challenge for Coast Guard.** The Coast Guard is weathering software glitches in its efforts to roll out a new modernized communication system by 2006. **"The software, which ties it all together ... has been a significant challenge for us and the contractor," said Cmdr. Ed Thiedman, assistant program manager for the project. "We have been focusing on**

immediate issues at hand ... as we get closer, we will start talking about full production completion by 2006 and if that is attainable." In September 2002, the Coast Guard awarded a contract to develop and implement a modernized communication system called Rescue 21. Under the agreement, two initial Coast Guard locations were to test with "full functionality" the software system by September of this year, according to a General Accounting Office report issued in late September. In July, the Coast Guard postponed the testing due to software problems with integrating commercial technologies into a software package that would enhance the agency's capability to assist and find boaters in distress, among other activities, said Thiedman. **Rescue 21, which has been in the works since 1997, is to be a short−range communication system with VHF−FM radios, communication towers as well as hardware and software at operation centers.**
Source: http://www.govexec.com/dailyfed/1103/111003tdpm2.htm

[Return to top]

Emergency Services Sector

23. *November 07, Gambling Magazine* — **Casinos expected to deliver emergency plans. Nearly half of Nevada's hotel−casinos have complied with a new state law requiring them to file emergency response plans with the state and local police and fire departments.** Jerry Bussell, chairman of the Nevada Homeland Security Commission, said that compliance is rapidly approaching 50 percent and is expected to approach 100 percent within two weeks. Most Nevada hotel−casinos missed the October 31 deadline for filing emergency response plans because of ambiguous compliance requirements and concerns about the security of information, said casino executives who asked not to be named. **The issue arose after only 14 Nevada casinos met the deadline for filing the emergency plans. The new law says plans must include the location of emergency equipment and hazardous materials, an evacuation program and a description of internal and external access routes. The law was designed to let firefighters, police and other emergency responders know how the properties would react in the event of a terrorist attack or other disaster.** The law affects only resorts with more than 200 rooms, which would cover all casinos built in Clark County since 1989.
Source: http://www.gamblingmagazine.com/managearticle.asp?C=420&A=32 10

[Return to top]

Information and Telecommunications Sector

24. *November 10, Australian Associated Press* — **Hackers reach Australian Defense files.** Hackers have reportedly accessed top−secret files inside the Australian Department of Defense. "There have been three incidents in which an external security breach has led to unauthorized access to computer systems," Senator Hill had told an inquiry into computer security in the public service. According to the minister, the Defense Department also reported 13 cases since 2000 of its own staff trying to hack into computer systems without authorization. **A review of electronic security inside commonwealth agencies has reportedly uncovered a culture of theft and lax security inside the public service. The inquiry comes amid a series of thefts**

of computers containing classified information from a customs office at Sydney Airport and the Transport Department in Canberra. Submissions by the major departments to the Joint Committee of Public Accounts and Audit has found that more than 1600 computers have vanished since 1998. Senator Hill said three computers stolen in the past two years contained information classified as "secret", but they had been recovered and the risk to national security had been assessed as low, he told the inquiry in a memo.
Source: http://www.theage.com.au/articles/2003/11/10/1068329455162.h tml

25. *November 07, Government Computer News* — **Kansas auditors crack 1,000 passwords.** The Kansas Health and Environment Department has serious IT security and disaster recovery problems, the state's legislative auditor has found. **The auditors said they used password−cracking software to decipher more than 1,000 of the department's passwords−including several administrative passwords−or 60 percent of the total, in three minutes**. The department began fixing the security weaknesses and other problems found in its systems as soon as it learned of them, department secretary Roderick L. Bremby said in response to the report. "The department's anti−virus system was badly flawed, allowing computers to become infected with a large number of different viruses, worms and Trojan horses," said the report. "The department's firewall was poorly configured, creating several large holes in and out," the report said. **Auditors found that the department lacked or failed to enforce many basic security policies**, such as procedures for incident response, physical security, configuration documentation and former−user account deletion. They also found several major problems with security planning.
Source: http://www.gcn.com/vol1_no1/daily−updates/24132−1.html

26. *November 06, CNET News.com* — **Attempted attack on Linux kernel foiled. An unknown intruder attempted to insert a Trojan horse program into the code of the next version of the Linux kernel, stored at a publicly accessible database**. The public database was used only to provide the latest beta, or test version, of the Linux kernel to users of the Concurrent Versions System (CVS), a program designed to manage source code. **The changes, which would have introduced a security flaw to the kernel, never became a part of the Linux code and were never a threat**, said Larry McVoy, founder of software company BitMover and primary architect of the source code database BitKeeper, Thursday, November 6. An intruder apparently compromised one server earlier, and the attacker used his access to make a small change to one of the source code files, McVoy said. **The change created a flaw that could have elevated a person's privileges on any Linux machine that runs a kernel compiled with the modified source code. The recent incident raises questions about the security of open−source development methods**, particularly how well a development team can guarantee that any changes are not introducing intentional security flaws. While Microsoft code has had similar problems, closed development is widely considered to be harder to exploit in that way.
Source: http://news.com.com/2100−7355_3−5103670.html

Internet Alert Dashboard

Current Alert Levels

 AlertCon: 2 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 21 (ftp), 445 (microsoft−ds), 161 (snmp), 80 (www), 139 (netbios−ssn), 1433 (ms−sql−s), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *November 10, Houston Chronicle (TX)* — **Homemade fire bombs damage apartment offices. Arson investigators are on the scene of a deliberate fire at the management offices of a northwest Houston, TX, apartment complex. Five homemade fire bombs, fashioned by filling bottles with flammable liquid, were found outside the apartment offices.** The fire was reported just after 2 a.m. at the offices of the Southern Garden Apartments. It was extinguished quickly and did minimal damage to the office, firefighters said. Firefighters said some of the homemade devices evidently were tossed through the office windows to start the blaze. No one was injured in the fire. Arson investigators are hoping the unused fire bombs hold evidence that will lead them to the arsonist.
Source: http://www.chron.com/cs/CDA/ssistory.mpl/front/2213310

28. *November 10, CNN* — **U.S. embassy in Sudan to close temporarily. The U.S. Embassy in Khartoum, Sudan, will be closed through the week because of a threat about a possible al Qaeda attack against American interests in the country**, two senior State Department officials said Monday, November 10. According to a State Department message that officials said was sent to U.S. citizens in Sudan, "This action is the result of a threat to U.S. interests in Khartoum. The embassy hopes to resume normal operations next week." **U.S. officials have previously warned of possible terrorist activities targeting U.S. interests in northern Africa**. And the threat comes on the heels of a terrorist attack Saturday against an expatriate housing compound in Riyadh, Saudi Arabia, which followed a week of warnings by the State Department about a possible threat there. The U.S. Embassy in Khartoum was closed in 1996 and re−opened about a year ago because of ongoing Sudanese support in U.S. efforts against terror and the emergence of peace talks between the Khartoum government and the country's southern rebels. The embassy is run by a charge d'affaires.
Source: http://edition.cnn.com/2003/WORLD/africa/11/10/sudan.embassy /

29. *November 10, Associated Press* — **IAEA says "no evidence" Iran is making nukes. A confidential United Nations nuclear agency report from the Vienna−based International Atomic Energy Agency (IAEA) has found "no evidence" to back U.S. claims that Iran tried to make atomic weapons, but it cannot rule out the possibility because of past cover−ups by Tehran,** diplomats told the Associated Press on Monday. In Moscow, a top Iranian official said his country is temporarily halting its uranium enrichment program and has agreed to tougher UN inspections. **Under international pressure, Iran recently gave the agency what it said was a complete declaration of its nuclear activities just days ahead of an October 31 deadline. On Monday, it also handed over two letters pledging to sign an additional agreement throwing open its program to inspection on demand by agency experts and announcing it had suspended uranium enrichment.** The concessions were announced in Moscow by Hasan Rowhani, the head of Iran's powerful Supreme National Security Council.
Source: http://www.foxnews.com/story/0,2933,102627,00.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP